Remarks

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. Claims 1, 3-4, and 9 have been amended. Claims 31-38 stand withdrawn. Claims 1-30 and 39-40 are now pending in the application. Replacement sheets containing formal drawings are submitted under separate cover with the declaration that no new matter is added. It should be noted that the MPEP does not explicitly require this declaration for replacement drawings meant only to replace informal drawings, but only for a replacement specification.

ARGUMENT

Claims 1-5 have been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. This rejection is respectfully traversed and Claims 1-5 are believed allowable based on the above amendments and following discussion.

Claim 1 is amended to explicitly recite that the data block is received in a data stream. Claim 3 is amended to recite the necessary condition for requiring a source of said portion of said payload. This necessary limitation for an embodiment of the invention is clearly described in the specification, at least at page 26, lines 12-16. When only one source circuit is used in the system, then the source need not be part of the data-stream identifier. Claim 3 recites limitations to handle both cases. Claim 4 is amended to remove the "necessary" language.

Claims 9-16 are rejected under 35 U.S.C. 112, second paragraph as being incomplete for omitting essential steps. This rejection is respectfully traversed and claims 9-16 are believed allowable based on the above amendments and foregoing and following discussion.

The Examiner asserts that a data block and a decrypted data block are not different. While the distinction is subtle, these two elements are not the same. For instance, some encryption and decryption schemes may insert or omit certain portions of the data block. An encrypted data block may include header information providing decryption keys or clues as to

which keys to use to decrypt. A decrypted data block defines a data block that has been previously encrypted and then decrypted. It will be apparent to one of ordinary skill in the art that the decrypted data block may contain information about the decryption or encryption engine. The decrypted data block may not be identical to the original unencrypted data block due to some loss of data during encryption and decryption or the addition of header information. Since Cooper et al. do not teach using data blocks that have been previously decrypted, the reference does not teach or suggest all of the elements of Applicants' claimed invention.

The actual step of encrypting and decrypting the data block is outside of the scope of Claim 9 because it is to take place in another component of the system which is not explicitly claimed. For instance, systems which use data retrieved from the Internet do not necessarily *claim* the Internet as an element of the claimed invention. In order to protect the Applicants' invention from infringement, excessive steps taken outside the claimed component are omitted from the Claim. However, it will be apparent to one of ordinary skill in the art that receiving a never-encrypted data block is not the same as receiving a data block that has previously been encrypted and then decrypted. The prior art teaches various methods for distributing software trials, but does not teach the claimed methods as acting on data that was previously encrypted or decrypted. Thus, Claims 9-16 are believed allowable and the Examiners interpretation of the term decrypted data block as a mere data block is incorrect.

Claims 9-16 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,757,908 to Cooper et al., (hereafter, "Cooper et al."). This rejection is respectfully traversed and Claims 9-16 are believed allowable based on the above amendments and the foregoing and following discussion.

Generally, Cooper et al. teach a system for enabling a file or software application which has been locked from the user. Cooper et al. teach an apparatus for securing access to particular files which are stored in a computer-accessible memory media. A plurality of files is stored in a computer accessible memory media, including at least one file previously encrypted by the vendor, and at least one unencrypted file. For each encrypted file, a *preselected portion of the file* is recorded in memory, a decryption block is generated which includes information which can be utilized to decrypt the file, and the decryption block is incorporated in the file in lieu of the *preselected portion* which has been recorded in memory. This entire file is then distributed to the

user. Cooper et al. does not teach a system which receives a decrypted data block and then replaces a portion of a decrypted data block and then re-encrypts the data block after setting a flag and sending to a receiving module.

In contrast, Applicants' invention recites a system for transmitting a data stream made up of data blocks, where a data block portion of a payload may be replaced with a tag indicating whether a decryption key is necessary to decode the data block. The data blocks of a given data stream may contain disparate protocols and be routed to one or more application decoders. Further, the sending device and receiving device may negotiate for a session key to decrypt the decryption keys, thereby enabling additional security to the data stream as is passes through the data safeguarding device. This negotiation is specifically claimed in the provisionally withdrawn claims.

Cooper et al. teach a system where only one portion of a file is encrypted to protect it from being accessed by a user upon a user request to access the file. An operating system level file management program determines whether the user is authorized to access the file and supplies the decryption key. Cooper et al. teach supplying the key by the vendor. Cooper et al. do not teach or suggest a *decrypted data stream* received from a source device, but merely a file drawn from media.

As described in the specification, and recited in the claims, Applicants' invention safeguards data within a device and forwards data of varying protocols to appropriate application decoders. If a data stream contains both audio and video data blocks, the data blocks from the received data stream may be sent to different application decoders based on their protocol, i.e., audio vs. video formats. Applying the teachings of Cooper et al. to Applicants' invention will result in an operating system level decoder for files and not a safeguarding device that may be implemented in hardware, software, or firmware that receives transmitted data streams without user request.

The Examiner asserts that Cooper et al. disclose all elements of the claims. The independent claims have been amended to more clearly recite that the sending system, received a decrypted data block and then re-encrypts at least portions of the data block before sending the encrypted data to the second system, i.e., the application decoder module. This encrypting of the data is a second encrypting, or *re-encrypting*. The data block is not received in an encrypted

mode and then merely passed through to the second system. It has been first decrypted. After decrypting by the first device, a portion of the payload may be replaced. At least a portion of the data block is encrypted before transmitting to the second device. Cooper et al. do not teach or suggest this decrypting or re-encrypting. Thus, Claims 9-16 are allowable as amended.

Cooper et al. do not teach a method to re-encrypt a decrypted data stream, but only a method to decrypt a pre-encrypted file on a media device. In contrast, Applicants' claimed invention receives a decrypted data stream and encrypts the payload portion of the data blocks in the data stream before sending them to one or more application decoders. The PCX and application decoders may be separate devices, circuits or modules, or they may be part of the same device. Regardless, the PCX and application decoders are part of an overall data safeguarding system. Cooper et al. teach that the encryption occurs on a vendor system and decryption occurs on a user system.

Claims 1-8, 17-30 and 39-40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 5,572,442 to Schulhof et al. (hereinafter "Schulhof et al.") in view of Cooper. This rejection is respectfully traversed and Claims 1-8, 17-30 and 39-40 are believed allowable based on the above amendments and the following discussion.

Schulhof et al. teach a distribution system for audio materials including a portable audio storage. Schulhof et al. teach that an encrypted data steam may be received from an input program signal. The data stream is decrypted, demodulated and decoded as necessary so that it can be stored on the portable storage device. However, once decrypted and stored, the data is susceptible to unauthorized access and manipulation. There is no guarantee that the stored data will maintain its integrity. In contrast, Applicants' invention passes the encrypted data blocks through a safeguarded system without storing them unprotected on a media device.

Combining the teaching of Schulhof et al. and Cooper et al. will not result in Applicants' claimed invention. If Cooper et al. were to retrieve data from the Schulhof et al. portable storage, it is the equivalent of retrieving an open data stream and not a decrypted data stream. Schulhof et al. do not suggest that the portable storage device stores anything other than the original unencrypted data stream. Schulhof et al. merely suggest that the data might be received in an encrypted format and that decrypting, decompressing and decoding take place as necessary. This teaching implies that the data stored on the portable media device is placed in its original state,

and accessible to any process having access to the device and thus susceptible to being read by, or modified by, any unauthorized system or device.

Further, combining the two references is improper as Cooper et al. teach installing trial software and Schulhof et al. teach distributing audio and video programming. There is no motivation to combine these teachings. Cooper et al. do not teach or suggest that their process may use audio and video programming, but only software code. Cooper et al. also teach using pre-selected encrypted portions of software. Cooper et al. teach that the software is received as reversibly functionally limited software. The pre-selected portions are received by the user in an encrypted state. Combining the teachings of Schulhof et al. would result in Cooper et al. receiving unencrypted and wide open software code which would negate the purpose of having functionally limited software distributed to users. Thus, the combination of the references is improper and Claims 1-8, 17-30 and 39-40 are believed allowable.

Thus, for the foregoing reasons, all claims remaining in the application are now allowable.

CONCLUSION

In view of the foregoing, Claims 1-30 and 39-40 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 7 Dec 2005

Joni D. Stutman-Horn
Patent Attorney
Intel Corporation
Registration No. 42,173
(703) 633-6845

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026